ASP Privacy & Security Policies

Access

How does your system ensure that only authorized users have access to only minimum necessary information?

The practice's administrator sets the access level for each user. Access is provided by role and view only/edit and update. Confidential chart access also allows the administrator to limit the access to individual patients in addition to role-based access.

Authorization

How does your system authorize users to access information?

Users are provided a user ID and initial password by the practice's security administrator. The security administrator also determine the password rules. Upon initial access the user is prompted to change their password and must continue to maintain their password consistent with the rules set in the system by their practice's security administrator. As mentioned above, access may also be limited to certain patients.

Authentication

How does your system ensure that the person accessing the system is who they say they are?

Via the user ID and password. Device based authorization such as key card, finger print, etc may also be used by the customer but is used in conjunction with the device and not the Sevocity application.

Audit

What audit procedures are in place that will promote transparency and compliance with access, use, and disclosure requirements?

All audit features required by ONC-ATCB and CCHIT 2011 are included. These features include, but are not limited to:
* Security Audit report
* User Creation report
* Access by User and by Chart
* Full audit trail within every encounter

Secondary Uses of Data

How does your system ensure that the use and disclosure of information is limited to appropriate and approved users?

The ability of a user to export PHI is controlled as part of the user's access level. In addition, a report is available on all exported PHI. Exported PHI is automatically encrypted and the user must password protect the PHI.

Data Ownership

Where is the data stored and who owns the data?

The data is stored in our Tier IV Data Center with triple redundancy. The practice owns the data and we never provide data (even de-identified data) to anyone without the practice's written permission.

Sensitive Protected Health Information

Sensitive health information refers to select protected health information (PHI). Federal and state laws impose heightened privacy and security requirements upon the disclosure of certain types of PHI that may be considered particularly private or sensitive to a patient such as genetic information, psychotherapy notes, substance abuse treatment records, etc.

Vendor did not provide additional information.

Yes	No	
☑	☐	*Does your system have the ability to identify PHI that is sensitive?*
		If yes, explain: Sevocity has a Confidential Blank Note.
☑	☐	*Does your system have the ability to prohibit sensitive PHI from being shared electronically?*
		If yes, explain: The Clinic determines who can see the data.
☑	☐	*Does your system have the ability to break the glass (Break the glass refers to the ability to obtain health information in emergency situations where consumer consent has not been granted)?*
		If yes, explain: Sevocity does have the ability to break the glass.

Consumer Accounting of Disclosures

How does your system generate reports for consumer of access to their records?

A chart access report is available.

Secondary Data Use

Does your EHR system have provisions which allow the EHR vendor to extract a Limited Data Set of patient information to use for research purposes by the EHR vendor or a third party, if the practice agrees to participate in a study?

Yes, we can extra data into an SQL file and provide the data schema.